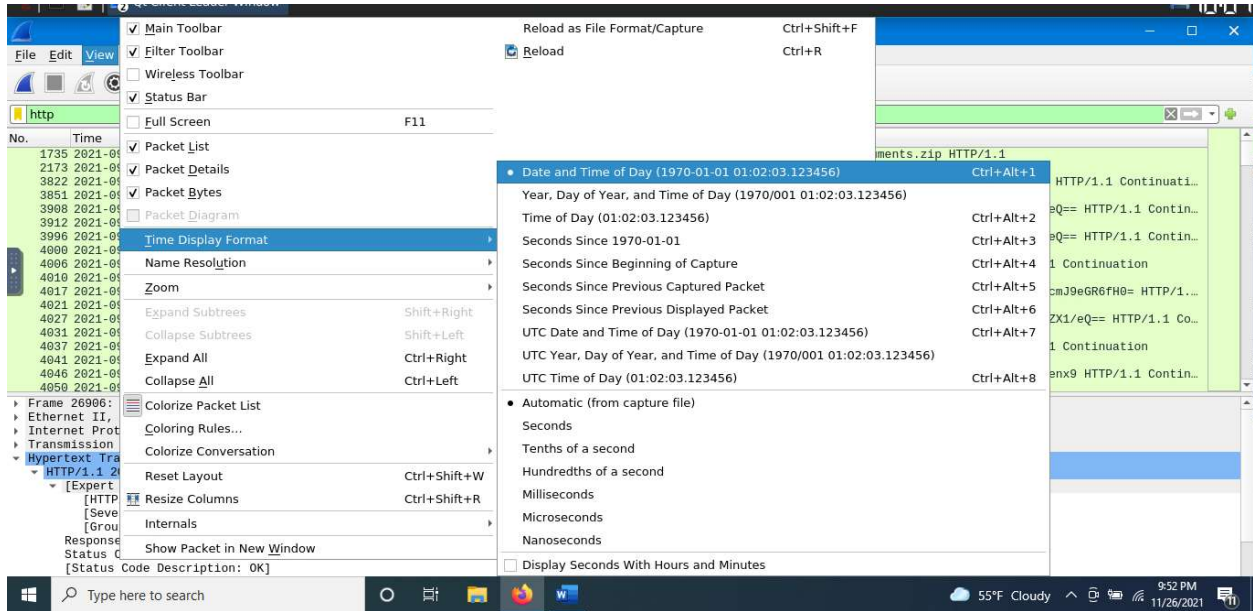


Tryhackme Carnage

<https://tryhackme.com/room/c2carnage>

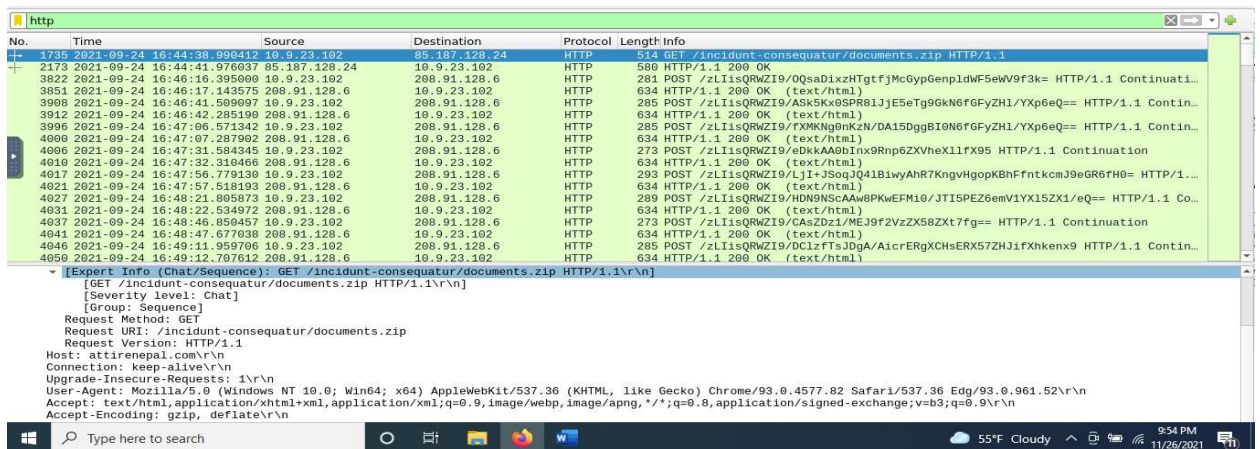
All the packet analysis will be done using wireshark.

- 1 Apply **http** as a filter and the go to **view** menu and then go to **Time Display Format** and chose first option



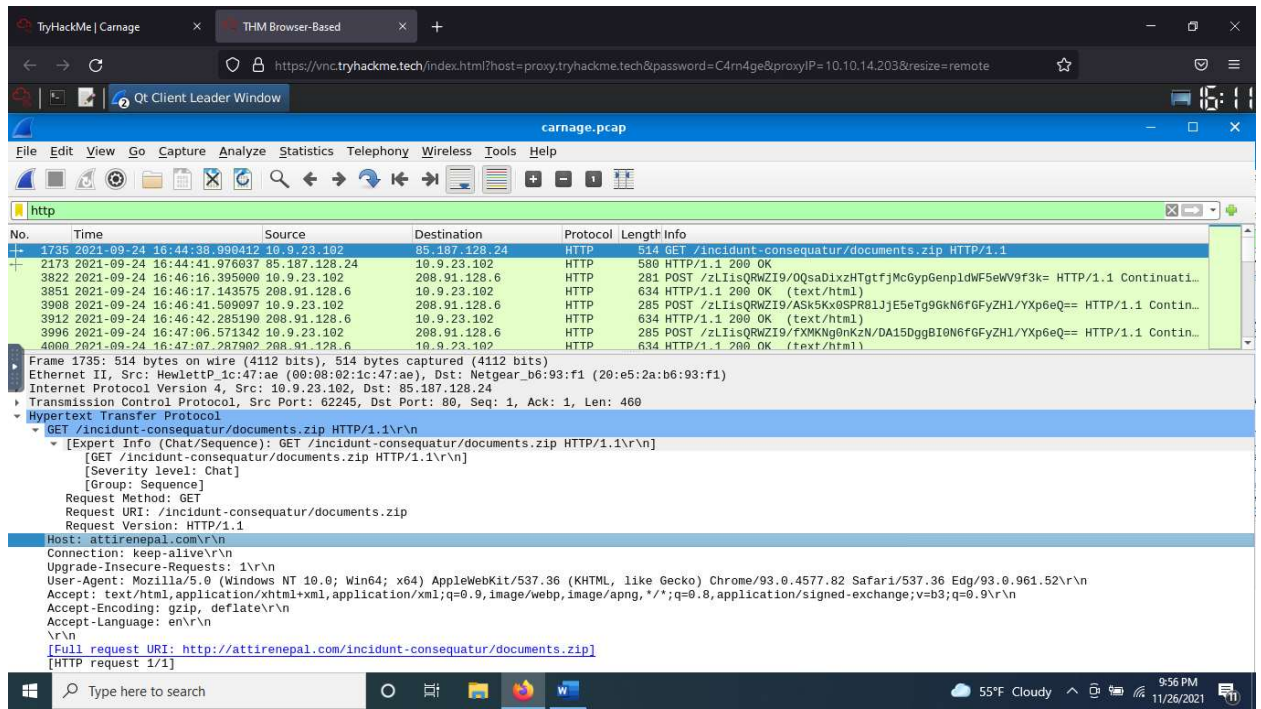
2

By clicking on first http packet we can view the details.



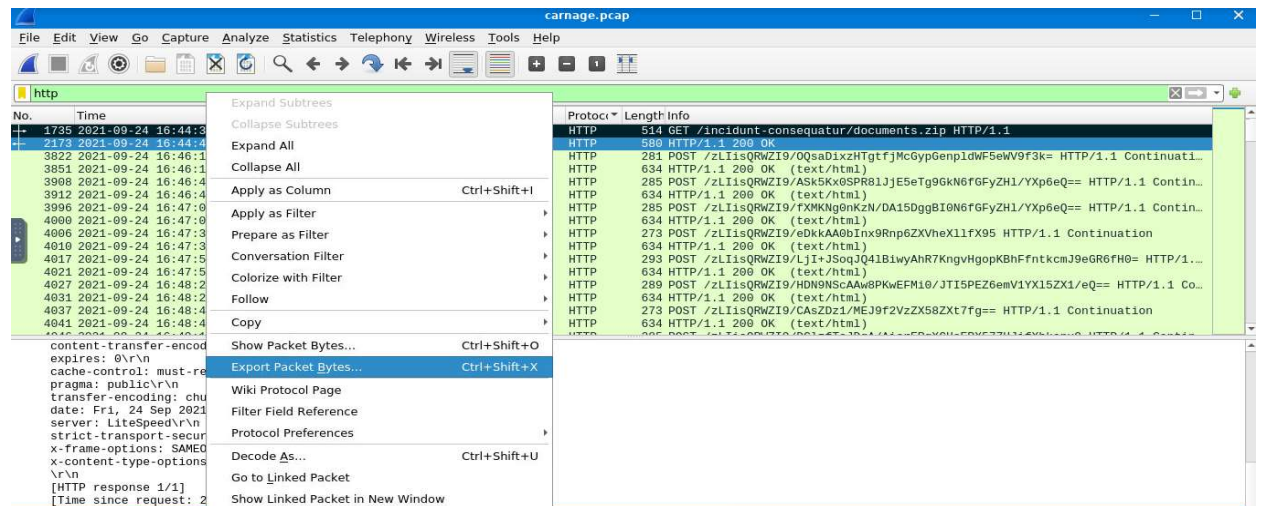
3

On the first traffic. By clicking on **Hyper Text Transfer Protocol** we can then view the **Host:** header and get our answer.



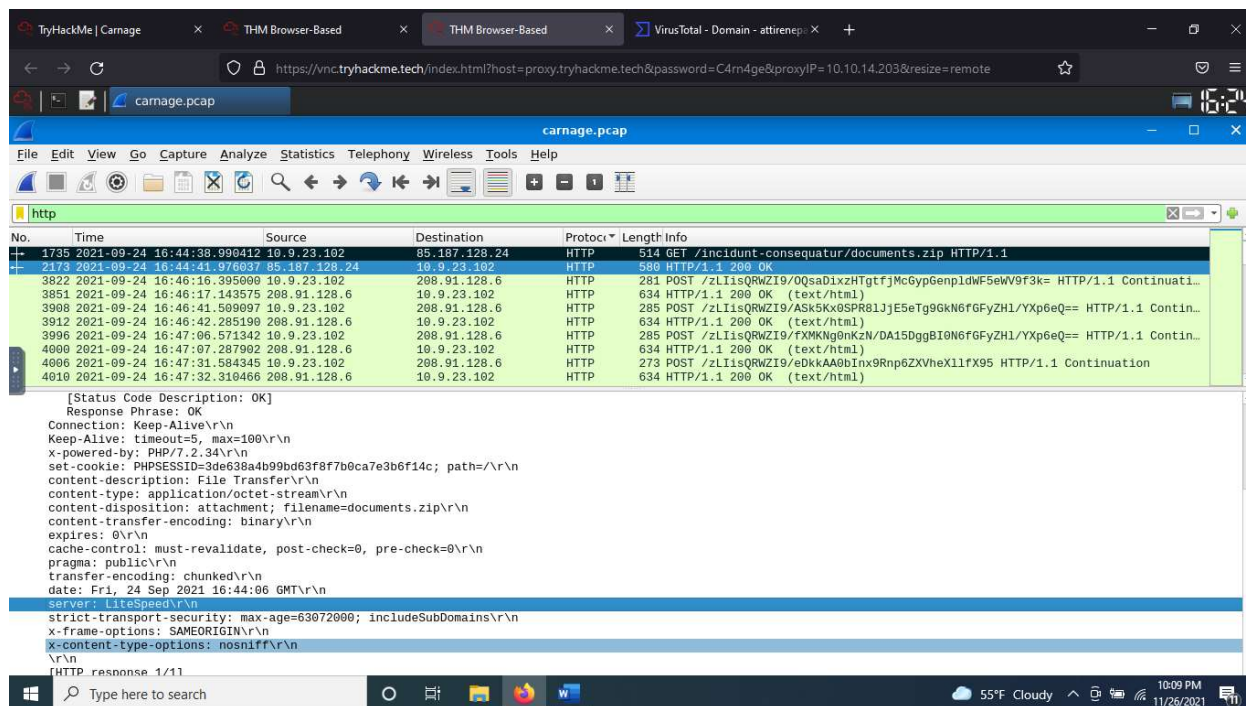
4

We can simply right click and use **export packet bytes** option and download it and unzip it . It is not the recommended method. If u can help me on how to view it without exporting and unzipping it.



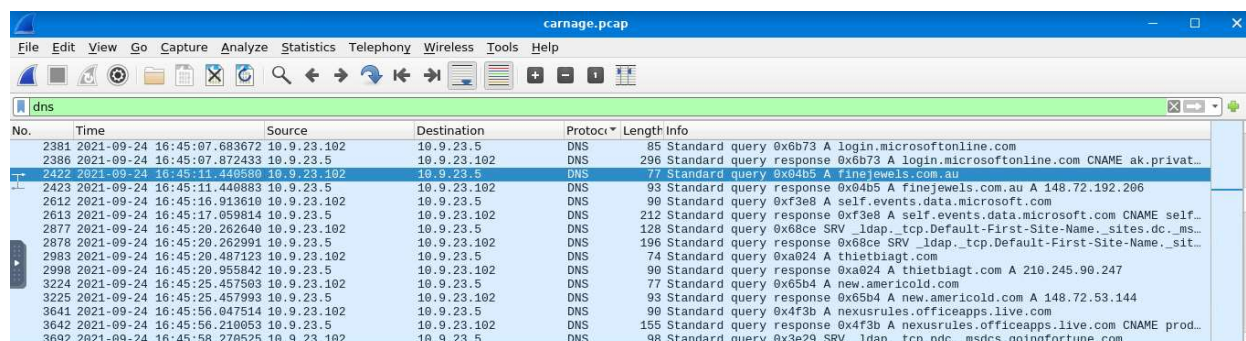
5 & 6

For server info. Go to the response packet and view **Hypertext Transfer Protocol** and under it there is **server** header and copy the value of it for question number 5 and for question number 6 look at **x-powered-by** header.



7

By setting filter to **DNS** and looking at the time range given in hints we can get the domain names



8 For it I search the domain at virustotal.com and in details tab view the registrar info and got the answer.

finejewels.com.au

2021-11-08 36 / 60 MS Excel Spreadsheet 16c9f2c4f5a5305d3ff433fad7f85ed0.viobj

Historical Whois Lookups

Last Updated	Registrar	Registrant
- 2021-09-28	-	-
<p>Name Server: NS21.DOMAINCONTROL.COM NS22.DOMAINCONTROL.COM DNSSEC: unsigned Domain Status: clientDeleteProhibited https://afilias.com.au/get-au/whois-status-codes#clientDeleteProhibited clientUpdateProhibited https://afilias.com.au/get-au/whois-status-codes#clientUpdateProhibited serverRenewProhibited https://afilias.com.au/get-au/whois-status-codes#serverRenewProhibited Last Modified: 2021-07-13T22:00:36Z Registrar Name: GoDaddy.com LLC trading as GoDaddy.com Registrant Contact ID: d8a24963e64a68b9 Registrar WHOIS Server: whois.auda.org.au Eligibility Type: Partnership Tech Contact ID: CR237092801 Registrant Contact Name: 8db7927a45d4122d Registry Domain ID: D40740000002016952-AU Registrant ID: 2144b3325d0a7a5d Registrant: ec6b0cad9c9a39f Domain Name: FINEJEWELS.COM.AU</p>		
+ 2019-12-27	-	-

9

By going to conversation menu which is under statistics I manually check the IP and found the ip address and check it in virus total

185.106.96.158

6 / 90

6 security vendors flagged this IP address as malicious

185.106.96.158 (185.106.96.0/22)
AS 35913 (DEDIPATH-LLC)

Community Score

DETECTION DETAILS RELATIONS **COMMUNITY 3**

Comments

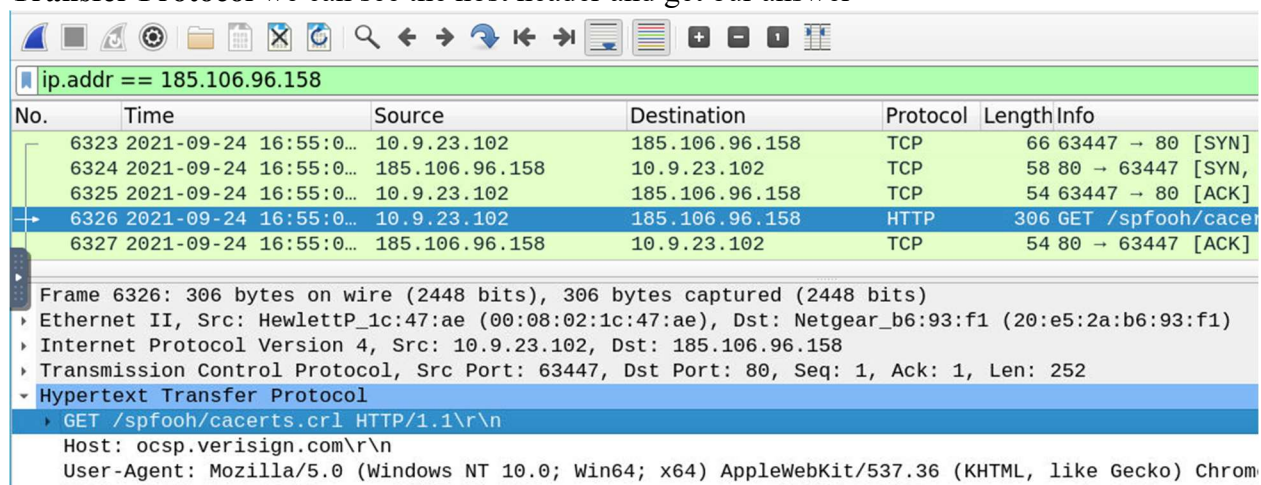
drb_ra
1 month ago

Cobalt Strike Server Found
C2: HTTPS @ 185[.]106[.]96[.]158:8888
C2 Server: survmeter[.]live/gscp[.]R/185[.]106[.]96[.]158/gscp[.]R/

10.9.23.102	185.106.96.158	1973	1319k
10.9.23.102	52.109.88.34	19	8352
10.9.23.102	52.109.88.178	20	8806
10.9.23.102	52.98.168.178	1008	616k
10.9.23.102	37.252.0.102	349	232k
10.9.23.102	104.83.84.137	9074	10M
10.9.23.102	23.111.114.52	18002	15M
10.9.23.102	52.182.143.211	25	8212
10.9.23.102	54.243.45.255	46	16k
10.9.23.102	50.16.239.65	520	178k
10.9.23.102	108.177.15.28	79	4766
10.9.23.102	173.255.233.87	26	1812
10.9.23.102	74.125.128.108	21	1182
10.9.23.102	64.29.151.102	18	1166
10.9.23.102	188.125.73.25	14	788

10

By setting the first IP as a filter and opening an http protocol and under **Hypertext Transfer Protocol** we can see the host header and get our answer



ip.addr == 185.106.96.158


No.	Time	Source	Destination	Protocol	Length	Info
6323	2021-09-24 16:55:0...	10.9.23.102	185.106.96.158	TCP	66	63447 → 80 [SYN]
6324	2021-09-24 16:55:0...	185.106.96.158	10.9.23.102	TCP	58	80 → 63447 [SYN,
6325	2021-09-24 16:55:0...	10.9.23.102	185.106.96.158	TCP	54	63447 → 80 [ACK]
6326	2021-09-24 16:55:0...	10.9.23.102	185.106.96.158	HTTP	306	GET /spfooh/cacei
6327	2021-09-24 16:55:0...	185.106.96.158	10.9.23.102	TCP	54	80 → 63447 [ACK]

Frame 6326: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits)

- Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
- Internet Protocol Version 4, Src: 10.9.23.102, Dst: 185.106.96.158
- Transmission Control Protocol, Src Port: 63447, Dst Port: 80, Seq: 1, Ack: 1, Len: 252
- Hypertext Transfer Protocol
 - GET /spfooh/cacerts.crl HTTP/1.1\r\n
 - Host: ocsp.verisign.com\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom

11 and 12

Searching for the IP address and going to community tab of virustotal gives us the answer.




× Community Score ✓

185.106.96.158 (185.106.96.0/22)
AS 35913 (DEDIPATH-LLC)


DETECTION DETAILS RELATIONS **COMMUNITY 3**

Comments ⓘ



drb_ra
1 month ago

Cobalt Strike Server Found
C2: HTTPS @ 185[.]106[.]96[.]158:8888
C2 Server: survmeter[.]live[.]gscp[.]R/185[.]106[.]96[.]158[.]gscp[.]R/




× Community Score ✓

185.125.204.174 (185.125.204.0/22)
AS 25369 (Hydra Communications Ltd)

DETECTION DETAILS RELATIONS **COMMUNITY 2**

Comments ⓘ



drb_ra
2 months ago

Cobalt Strike Server Found
C2: HTTPS @ 185[.]125[.]204[.]174:4444
C2 Server: securitybusinpuff[.]com/jquery-3[.]3[.]1[.]min[.]js,185[.]125[.]204[.]174/jquery-3[.]3[.]1[.]min[.]js

13 and 14

use **http.request.method ==POST** as a filter and open the first packet and go under **Hypertext Transfer protocol** and in **host:** header one can see the domain name and get answer for 13 and for 14 copy and paste the character between first two / or the first directory after /.

http.request.method == POST						
No.	Time	Source	Destination	Protocol	Length	Info
3822	2021-09-24 16:46:1...	10.9.23.102	208.91.128.6	HTTP	281	POST /zLIisQRWZI9/0QsaD1xzHTgtfjMcGypGenp1
3908	2021-09-24 16:46:4...	10.9.23.102	208.91.128.6	HTTP	285	POST /zLIisQRWZI9/Ask5Kx0SPR81JjE5eTg9GkN6
3996	2021-09-24 16:47:0...	10.9.23.102	208.91.128.6	HTTP	285	POST /zLIisQRWZI9/fXMKNg0nKzN/DA15DggBI0N6
4006	2021-09-24 16:47:3...	10.9.23.102	208.91.128.6	HTTP	273	POST /zLIisQRWZI9/eDkAA0bInx9Rnp6ZXVheX11
4017	2021-09-24 16:47:5...	10.9.23.102	208.91.128.6	HTTP	293	POST /zLIisQRWZI9/LjI+JSoqJQ41BiwyAhR7Kngv

Frame 3822: 281 bytes on wire (2248 bits), 281 bytes captured (2248 bits)
Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
Internet Protocol Version 4, Src: 10.9.23.102, Dst: 208.91.128.6
Transmission Control Protocol, Src Port: 63385, Dst Port: 80, Seq: 1, Ack: 1, Len: 227
Hypertext Transfer Protocol
POST /zLIisQRWZI9/0QsaD1xzHTgtfjMcGypGenp1dWf5eW9f3k= HTTP/1.1\r\n
Host: maldivehost.net\r\n
Content-Length: 112\r\n

15

By going to first packet to the maldivehost.net. we can see the answer on the Frame details and also in above ss.

http						
No.	Time	Source	Destination	Protocol	Length	Info
3851	2021-09-24 16:46:17.143575	208.91.128.6	10.9.23.1...	HTTP	634	HTTP/1.1 200 OK (text/html)
3908	2021-09-24 16:46:41.509097	10.9.23.102	208.91.12...	HTTP	285	POST /zLIisQRWZI9/Ask5Kx0SPR81JjE5eTg9GkN6f
3912	2021-09-24 16:46:42.285190	208.91.128.6	10.9.23.1...	HTTP	634	HTTP/1.1 200 OK (text/html)

Frame 3822: 281 bytes on wire (2248 bits), 281 bytes captured (2248 bits)

16

Then again right click on the packet and go to follow and follow HTTP stream and in the response u can see the server info

The screenshot shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets. The middle pane shows the details of the selected packet (Frame 3908), including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The bottom pane shows the raw packet data. A context menu is open over the selected packet, with the 'Follow' option highlighted. The 'Follow' submenu is also visible, showing options for following the TCP Stream, UDP Stream, TLS Stream, HTTP Stream, HTTP/2 Stream, and QUIC Stream. The 'HTTP Stream' option is selected, and the response data is displayed in the bottom pane, showing the full request URI and the response status (200 OK).


```

POST /zLIisQRWZI9/ASK5Kx0SPR8lJjE5eTg9GkN6fGFyZHl/YXp6eQ== HTTP/1.1
Host: maldivehost.net
Content-Length: 112

Dw8YBxsEGmYFAAEJfR4NQkMmLTyqZDk5KyQmOyRGQglxEB04Lzk/
EyYrMi1hOT8vIyM7IhcNPzs0KjguFxgkLSIiJCxFrgwFagIIDQUZGBoFD0JFHTTP/1.1 200 OK
Date: Fri, 24 Sep 2021 16:46:40 GMT
Server: Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4
X-Powered-By: PHP/5.6.40

```

17 and 18

By using **dns** filter and searching for the term api we can see an api. dns query and get both of our answer.

dns						
No.	Time	Source	Destination	Protocol	Length	Info
...	2021-09-24 16:59:35.543973	10.9.23.5	10.9.23.1...	DNS	166	Standard query response 0x15e9 SRV _ldap._tcp.
...	2021-09-24 16:59:35.660009	10.9.23.102	10.9.23.5	DNS	98	Standard query 0x73c5 SRV _ldap._tcp.pdc._msdc
...	2021-09-24 16:59:35.660368	10.9.23.5	10.9.23.1...	DNS	166	Standard query response 0x73c5 SRV _ldap._tcp.
...	2021-09-24 17:00:04.093354	10.9.23.102	10.9.23.5	DNS	73	Standard query 0xc92c A api.ipify.org
...	2021-09-24 17:00:04.233864	10.9.23.5	10.9.23.1...	DNS	299	Standard query response 0xc92c A api.ipify.org

19

By using **smtp** filter we can see a from mail and going inside the packet we can get our answer

smtp						
No.	Time	Source	Destination	Protocol	Length	Info
...	2021-09-24 17:02:45.698448	185.4.29.135	10.9.23.1...	SMTP	75	S: 220 mail.mailfa.com
...	2021-09-24 17:02:45.964203	10.9.23.102	185.4.29.1...	SMTP	68	C: Pass: ZGluYW1pdA==
...	2021-09-24 17:02:45.964344	10.9.23.102	185.4.29.1...	SMTP	70	C: EHLO localhost
...	2021-09-24 17:02:46.192228	185.4.29.135	10.9.23.1...	SMTP	110	S: 250-mail.mailfa.com SIZE 30000000 AUTH L
...	2021-09-24 17:02:46.198191	185.4.29.135	10.9.23.1...	SMTP	74	S: 235 authenticated.
...	2021-09-24 17:02:46.778017	10.9.23.102	185.4.29.1...	SMTP	86	C: MAIL FROM:<farshin@mailfa.com>
...	2021-09-24 17:02:46.778150	10.9.23.102	185.4.29.1...	SMTP	66	C: AUTH LOGIN

20

By using **smtp** as a filter wireshark displays the total number of packet related to it in the bottom and we can get our answer

Simple Mail Transfer Protocol: Protocol	Packets: 70873 · Displayed: 1439 (2.0%)	Profile: Default
---	---	------------------